NMAO Fleet Information Technology Security Policy 1.1
Marine Operations Center
November 4, 2005

1. PURPOSE: This policy guides shipboard network administrators in implementing and using information technology (IT) security effectively and productively. This policy provides for a foundation that protects the fleet shipboard networks and resources from the risks associated in data collaboration on a network. The first goal of this policy is to ensure that authorized users have access to the network resources they require in order to perform their duties. The second goal is that security is maintained at an appropriate level to protect these resources from unauthorized access and insure availability.

2. SCOPE: Each shipboard network will have administrators to perform information systems security implementation through installation and configuration of the network's system resources. The shipboard network system is mission critical and provides all computer services needed by the ship while in port and under way. These services include scientific data acquisition and processing, general administrative support, and network connectivity. Shipboard networks are no longer isolated from the NOAA wide area network and public Internet during the field seasons and therefore are exposed to additional risk than in the past. The ship's network regularly hosts NOAA officers and crew. Additional scientists and crew are given clearance by NOAA to participate in cruises. They support the ship's scientific and survey mission and are given controlled access to required network resources. This policy provides guidance to assist the shipboard administrators in the endeavor of implementing IS security on their assigned ships.

3. POLICY

3.1. ACCESS AUTHORIZATION FOR FILES DATA: Files stored on network servers must only be accessed by approved users that are grouped by access levels. The ship network administrator, with input from the ship's commanding officer, will classify which files are to be accessed by which access level. The level of the user's access to files will range from read only, modify, or full control. The assigned chief for scientific data collection will supply the required access rights for members of the scientific party. Review of approved access levels will occur:

* Upon the arrival of new command, crew, or scientific personnel.
* Upon the departure of command, crew, or scientific personnel.
* No less than once each year

Network administrators shall remove file access authorization for departing personnel, who will not require access in the future, within two working days of receiving notice from the command or the departure of a scientific party.

3.2. CONTROL OF SENSITIVE HUMAN RESOURCE DATA: Information which is sensitive or confidential must be protected from unauthorized access or modification. Users of sensitive human resource data must maintain the data on their assigned computers and not on network file servers. Users, with technical guidance from the ship network administrator, are responsible for controlling local access to the computer as well as the backup of sensitive data on the assigned computer. Created backups are then stored in a locked container and destroyed when no longer required.

3.3. PASSWORD CONTROLS: Assigned shipboard personnel who are given an NOAA individual email account that is not a guest or atsea account will also be given a ship network user name that matches the user's ID in the email address. For example, if the email address assigned is John.Smith@noaa.gov, then the network user name shall be John.Smith. The user is provided an initial network login password by the network administrator but forced to change to a user selected password using the following guidance:

* Passwords must be created that are consistent with the following criteria:

    (1) Passwords must have at least eight [**8**] non-blank characters;

    (2) At least one of the characters must be from the alphabet (upper or lower case);

    (3) Six of the characters may only occur once in the password (e.g., 'AAAAAAA1' is not acceptable, but 'A%rmp2g3' and A%ArmA2g3' are acceptable);

    (4) At least one of the characters must be a number [0-9] or a special character [e.g.,@,!,$,%,=,and *];

* Passwords MUST NOT include any of the following:

    (1) Names;

    (2) Words found in dictionaries;

    (3) Addresses or birthdays;

    (4) Common character sequences.

* Vendor-supplied default passwords, such as SYSTEM, Password, Default, USER, TEST, and [blank] must be replaced immediately upon implementation of a new system.

* Do not resuse a password that has been used any of the last 2 years or the last 8 times that the password was previously changed.

* Passwords are not to be displayed on or near the monitor.

* User passwords must be changed as follows:

    (1) At least every 90 days,

    (2) Immediately if discovered to be compromised or one suspects a password has been compromised,

    (3) Immediately if discovered to be in non-compliance with this policy, and

(4) On direction from management.

* At a minimum, system and administrative passwords must be changed annually prior to the beginning of the ship's field season.

** Network administrator will maintain the system and administrative passwords. These system and administrative passwords will not be shared with unauthorized personnel.*

3.4. CONTROL OF PASSWORD FILE: The vendor-supplied passwords and account numbers will be removed before a system is placed into operation. The password control file is the responsibility of the network administrator with access through an encrypted authorized password program. Each ship network administrator is licensed for one copy of Moon Software Password Agent software application**.** Password Agent is a secure password manager program that allows you to store all your passwords, secret notes and data snippets in a single, easy to navigate, and encrypted database. Use the application to manage the ship network passwords for the following minimum set of systems:

* Windows 2000/2003 Domain Administrator
* Netscape Enterprise Messaging System (NEMS)
* Sendmail Switch
* Cisco router access and enable password

Install Password Agent on a computer under the control of the network administrator and complete password entry records for all required systems. Send an email to the MOC Network Administrator at the email address nmao.it.security@noaa.gov and include the following information:

* Computer where Password Agent is installed.
* User name to access computer.
* Attach the PassEval.pwa file.

Upon receipt of the email the MOC Network Administrator will contact the ship's network administrator and receive the Password Agent password and the computer password for the supplied user name. Supply a hard copy of the Password Agent entries in a sealed envelope to the ship's Commanding Officer, or assigned representative, for storage in a locked container. Repeat notification process at least annually, as system passwords are updated or if the location of the computer hosting the ship's Password Agent program changes. Upon receipt of the outdated hard copy, the administrator inspects the sealed envelope insuring the envelope has not been tampered with before the contents are destroyed by use of an office shredder.

3.5. VIRUS PROTECTION: New viruses, worms and other malicious code are being released at an alarming rate. NOAA is licensed to deploy the McAfee Active Virus Defense Suite software. This software is capable of continuous monitoring and reporting malicious programs and is required to be installed on every NOAA PC to prevent contamination. Regularly updating virus definition (.DAT) files on all systems is essential to protecting IT resources from

compromise. McAfee VirusScan's Auto-update utility allows system administrators to schedule and manage the update process. Additional information on acquiring new virus definition files and the configuration of Auto-Update is located in ***Appendix 5.1***.

3.6. SECURITY PATCH MANAGEMENT: The term patch management describes the tools, utilities, and processes for keeping computers up to date with new software updates that are developed after a software product is released. The network administrator periodically will need to apply software updates, configuration changes, and countermeasures to eliminate vulnerabilities from the ship's network environment and mitigate the risk of computers being attacked. Service packs, hotfixes and security patches are updates to products to resolve a known issue or workaround. Moreover, service packs update systems to the most current code base. The most recent service packs for each Microsoft operation system (OS) can be found in the ship's Microsoft TechNet Subscription binder. All shipboard PCs with a Microsoft OS will be running the latest service packs. Individual hotfixes and security patches on the other hand shall be adopted on a case-by-case, "as-needed" basis. Guidance on the installation of hotfixes and security patches will be provided by the MOC Network Administrator, the NMAO Chief Information Officer (CIO), or the NOAA Computer Incident Response Team (NCIRT) through e-mail notifications.
If broadband internet access is available, then the ship network administrator shall use the Microsoft Windows Update site. The site hosts updates and patches for Windows operating systems and their components. Use the client PC's Internet Explorer browser to access the address, http://windowsupdate.microsoft.com, and the site will determine which patches haven't yet been installed on the system, let you select the patches desired, and then install them automatically.

3.7. SHORESIDE NETWORK CONNECTION: Access to a NOAA Facility provides a ship the ability to connect directly to the NOAA Wide Area Network (WAN). In order to protect the network security of the NOAA enterprise, the ship's network will meet the following requirements prior to establishing a direct connection to the NOAA WAN:

(1) Installation of the latest virus definition (.DAT) file on all systems and performance of a virus scan on each system.
(2) Installation of the latest critical operating system security patches.
(3) No external public Internet Service Provider (ISP) connections.

Other ship support sites and shipyards typically will offer a network connection through a commercial broadband ISP. A network router with firewall and Network Allocation Table (NAT) capabilities must be installed between the cable or DSL modem and the ship's network switch. The router is a separate hardware device from the modem. The ship's networked systems are protected by the NAT based router's ability to mask the IP addresses that are transmitted with the ship's outgoing internet traffic.

Future shipboard network capability will require the use of IPSEC supporting hardware to

establish a Virtual Private Network (VPN) tunnel between the ship and the NOAA Trusted Campus Network (TCN). A secure network connection to the TCN will provide the ship access to NMAO hosted network resources.

3.8. REPORTING AN INFORMATION SECURITY INCIDENT: An information security incident is something that can have a damaging effect on a computer or information system and related assets. Examples of incidents include:

* computer virus infections
* compromised passwords
* forged e-mail
* attempted or actual break-ins
* damage, disclosure, or loss of data
* denial of service
* theft
* misuse of information systems

Shipboard network administrators must provide an initial report by e-mail or voice communications to a MOC Network Administrator within 24 hours from when the incident is discovered. Information for a full written report must be sent within three working days of the known or suspected incident. Provide the following information so that a NOAA Form 47-43 is submitted by NMAO:

* Incident Date
* Incident Time
* Duration of Incident
* PC Description and IP Address of each Affected System
* If Malicious Software, the Virus Name
* Incident Description. Include affected system(s) or site(s), hardware and operating system, symptoms, connections with other IT systems that were active, actions taken, damage, and assistance needed.

Report incidents by e-mail using the following group email address:

nmao.it.security@noaa.gov

Use a system that is not affected by the incident. Do not discuss actual or suspected incidents with the press.

Report incidents by voice communications using the following telephone number:

(757) 650-0987

All initial voice comm reports will be followed up with an email that captures the above infomation so that an accurate NOAA Form 47-43 can be submitted. Use the telephone, not e-mail, to report an actual or suspected attack by an intruder. An intruder attack is only reported by using voice communications, never by e-mail.

Limit the extent of the incident. Steps include:

* Unplug the network connection. DO NOT restart or shutdown the system.

* Immediately start documenting the potential security problem and all system activities in a log book.
* If given guidance from MOC Network admin or NCIRT technician, reconnect to the network to monitor activity.
* Preserve evidence.

The resolution of the incident will require the cleaning of all infected media, restoring of data or programs, and returning the system to normal operation.

3.9. COMPUTER SECURITY AWARENESS TRAINING: New shipboard employees must complete the annually updated Computer Security Awareness Training course within three days of being assigned use of IT equipment. Course is available online at:

http://noaa.learnsecuritywith.us/access/login.asp

The ship will also maintain a standalone version of the course on board. Course is updated annually and a new course CD is distributed in February of each year. Annual review of this course is MANDATORY for all NOAA employees. All employees are required to complete the annual review of the course by March 31. MOC Operations will notify the ship's command if an individual is in danger of not completing the course by this date or there is no record of an newly assigned individual completing the course per the above guidance.

3.10. COMPUTER SECURITY AWARENESS TRAINING FOR CONTRACTORS AND TEMPORARY PERSONNEL: The Computer Security Awareness Training course is also required for all NOAA contractors, and temporary personnel. Temporary personnel includes visitors, guest workers, associates, etc., who plan to work at a NOAA site and use NOAA IT resources for more than a month." For those working less than a month, use this guidance: Ref DOC IT Security Policy and Minimum Implementation Standards, Section 3.13.1 ... The rigor of the training may vary depending on the risk of harm posed by the user – for example, a guest for two days may be provided a document of the system rules to sign acknowledging understanding and acceptance, whereas one month summer intern may be required to complete a Web-based training course. If a person is aboard less than a month and has a "guest" email account, then follow the above DOC guidance. If the person is given a noaa.gov email account, then follow the above DOC guidance and then send an eMail to the NMAO CIO with the person's NOAA email address and their estimated date of detaching from NOAA. This email address is:

nmao.it.security@noaa.gov

3.11. NEW NOAA REQUIREMENT TO DEPLOY THE STAT SCANNER NETWORK SECURITY TOOL: The is a new requirement and details will follow. The description of the software application follows:

STAT® Scanner Professional Edition performs a complete security analysis of Windows NT®, Windows® 2000/XP, Windows® Server 2003, Windows® 95/98/Me, Cisco® Routers and HP Printers using the most comprehensive vulnerability database on the market. STAT® Scanner is

Harris Corporation's network security tool that scans a computer network, looking for vulnerabilities that provide hostile intruders a way to compromise the system. With a few clicks of the mouse, the administrator can scan an entire network of computers and assess the vulnerabilities that exist on the network as determined by STAT Scanner's comprehensive vulnerability database. The database vulnerability assessment information is based on the knowledge of the STAT team of security engineers who have researched security advisories, knowledge base papers and professional security group articles to provide a single source of vulnerability information. STAT Scanner is updated several times a month to keep the user up to date with the latest threats from hackers. Additional information is located at the following site:

http://www.statonline.harris.com/solutions/faqs/professional_faq.asp

Future information on the deployment and administration of STAT Scanner will be located in ***Appendix 5.2***.

3.12. LOCK ADMINISTRATOR DESKTOP WHEN INACTIVE: An administrator will logoff the administrator account when not present at the computer or lock the computer by pressing CTRL+ALT+DELETE, and then select Lock Computer in the Windows Security dialog box. The "Windows logo key+L" shortcut can also be used to lock the computer. On the computer that the administrator regularly uses, the Windows screen saver will be configured for a five minute or less wait period and active password protection.

4. REFERENCES

4.1. U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards**,**
http://home.commerce.gov/DOC-IT-Security-Program-Policy.htm

4.2. NOAA NAO 212-13 and the IT Security Manual, 212-1300 as authorized by the NOAA Administrative Order 212-13,
https://www.csp.noaa.gov/policies/manual/212-1300.html
- and -
https://www.csp.noaa.gov/tea/index.html

5. APPENDIX

5.1. Configuring Auto-Update for NAI VirusScan 4.5.1 Open Scheduler or Console Program

5.1.1 Acquire New DAT Files

1. The following methods are used to receive new DAT Files:
   a. Go to site, http://vil.nai.com/vil/virus-4d.asp and download file, DAILYDAT.ZIP and unzip.
   b. Receive DAILYDAT.ZIP as an email attachment and unzip. Attachment size is about 2.3 Mb. Please send email request to: nmao.is.security@noaa.gov
   c. Access a client PC that has ran a new ####xdat.exe or sdat####.exe where #### is an NAI assigned number. Go to the following file to retrieve DAT files:
   C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

2. You can join a NAI New DAT email notification service by visiting the following link:
http://vil.nai.com/vil/join-DAT-list.asp

5.1.2 Configure Network File Share

1. Create the following Domain User, DATUSER, and configure as a Member Of Power Users. Assign a password.
2. Create a network file share and label it: NAIDAT.
3. Enter Sharing and Security for folder and select Security Tab.
4. Under Groups and User Names provide administrators full control and DATUSER read only access.
5. Place the following three files from the latest unzipped DAILYDAT.ZIP: CLEAN.DAT,

NAMES.DAT, SCAN.DAT.

5.1.3 Configure Client

1. Open VirusScan Console.
1. Double Click entry for AutoUpdate or Highlight this entry, right click and select properties.
2. Click on Schedule Tab.
3. Click Enable schedule.
4. Select Daily.
6. Select Enable randomization.
7. Click Progam Tab.
8. Now Select Configure Button.
9. Select Add Site.
10. Enter NOAA Ship in the Site Description Box.
11. Select Enable Site.
12. Select Retrieve Files From UNC Path
11. Enter (network share)\NAIDAT into the UNC Path field.
    Ex. \\10.49.29.30\share1\NAIDAT
12. Use DATUser login with password. Confirm password.
13. Click ok to close window.
14. Highlight the NOAA Ship Entry and Move it to the top of the list with the move up button.
15. Select Advanced tab.
16. Check "Update scanning engine if newer scanning engine exists.
17. Select OK button to return to Auto-Update Task properties screen.
18. Configuration is now complete, click ok to return to the Scheduler screen.
19. To update Dat Files right away, highlight AutoUpdate and select the Update Now button.